



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,366	10/14/2003	William Joseph Eakin	10018596-1	4386

22879 7590 11/09/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

D'AGOSTA, STEPHEN M

ART UNIT PAPER NUMBER

2617

DATE MAILED: 11/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

RECEIVED

NOV 09 2006

Technology Center 2800

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/685,366
Filing Date: October 14, 2003
Appellant(s): EAKIN, WILLIAM JOSEPH

Phil Lyren, Reg. #40,709
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10-9-2006 appealing from the Final Office action mailed 5-8-2006.

(1) Real Party of Interest

The real party of Interest is correct.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect *due to recent claim objections identifying novelty*. A correct statement of the status of the claims is as follows:

Claims 7-9, 10-11 and 18 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 2002/0069355	Garrison	06-2002
US 2002/0077077	Rezvani et al.	06-2002
US 6,763,091	Shimada	06-2004
US 5,333,152	Wilber	07-1994
US 6,665,396	Khoury et al.	12-2003
US 6,78,093	Obouchi et al.	09-2004
US 5,745,556	Ronen	04-1998
US 6,297,726	Yamazaki	10-2001
US 6,178,505.	Schneider et al.	01-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims (From the Final Office Action):

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-6, 12-17 and 19-31 rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison US 2002/0069355 and further in view of Rezvani et al. US 2002/0077077 **and** (Shimada **or** Wilber **or** Khouri **or** Obouchi **or** Ronen **or** Yamazaki).

As per **claims 1, 12, 19, 22 and 24-25 and 27**, Garrison teaches a method for communicating information from a private database to a wireless communication device (abstract, figure 1 and Para#33 teaches wireless communications), comprising:

receiving a private database access request from the wireless communication device, (figure 4a-b and Para#42 teaches Username/Password which uniquely ID's the user/device) ;

comparing the password with a security indicia, the security indicia associated with the wireless communication device (figure 3 teaches a Password table #55 which is checked as does figures 4a-b), and

communicating the information from the private database to the wireless communication device when the appliance ID corresponds to the security indicia (figures 4a-b teaches authenticating the user and sending the data if the user is verified) **but is silent on** the private database access request including **at least** an appliance identification (ID) that uniquely identifies the wireless communication device and

comparing the appliance ID with security indicia wherein verification of only the appliance ID is sufficient to authorize access to the private database.

Garrison teaches authenticating a user via username and password, as pointed out by the primary examiner above. Garrison discloses use of many different communications networks (see Para#33) and one skilled understands that this would encompass use of the Internet. Hence the client's device/computer would use TCP/IP addressing which would inherently uniquely identify the appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a database via communication means (Para#'s 108-111, 113 teaches cellular phone access, 121, 122 and 134). Furthermore, the examiner's response to arguments (see above) states that Rezvani discloses access to remote "systems" by only device ID/serial number (see Para's 2-7, 12, 16 and 18).

Shimada teaches using the telephone number of a device to register said device and connect to a network (abstract. Note that figure 1 shows the Internet being used).

Wilber teaches:

"If a carrier is detected at 236, a signal is sent to the local computer 52 which requests or prompts the local computer 52 to provide a **caller ID (eg. phone number)** and a password at step 242. The caller ID and password are verified at step 244, and if found appropriate a file transfer is executed at step 246" (C5, L58-62)

Khouri teaches:

In another embodiment, a database may be established to maintain specific caller priorities 66. ***Specific callers may be identified by the caller's telephone number 60*** or the caller may be asked to provide an access code or user ID.

In this embodiment, the database may identify the caller in order to establish their priority within the queue using their telephone number, password, or user ID. (C6, L54-65)

Obouchi teaches:

FIG. 3 is a graphical table illustrating exemplary contents in a collection of registered sentences for individual. Private information items that identify the user, such as the ID, name, telephone number and password of that user, are preferably appended to the collection of registered sentences for that individual. (C5, L56-61)

Ronen teaches:

Specifically, in these embodiments, before they are sent to the telephone company, the user's telephone number and a password known only to the user and to the telephone company, are encrypted with a public encryption key that is associated with only the telephone company. After authenticating the user by confirming the association between the decrypted telephone number and the password provided by the user, the ISP begins to provide the requested information and/or interactive services to the user. (C2, L62 to C3, L5)

Yamazaki teaches::

To make this possible, the pager uses a caller's telephone number as a password. (Abstract)

With further regard to claims 19 and 22 and 30-31, Garrison teaches use of password authentication and RF transmissions while Rezvani teaches use of an ESN number which reads on applicant's use of term "multiple use" (see claim 2 below as well) and transmitter/processor (see figure 1).

With further regard to claim 24, Garrison teaches a computer system/program executed on client and server (figures 2-3) with software logic shown in figures 4a-b)

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the private database access request including at least an appliance identification (ID) that uniquely identifies the wireless communication device and comparing the appliance ID with security indicia, to provide added security checking of both login/password and device ID.

As per **claims 2 and 13**, Garrison teaches claim 1/12, **but is silent on** wherein the appliance ID is multiple-use identification indicia that is included in all communications from the wireless communication device.

Rezvani teaches authenticating a user via an ESN number of a cellular phone (Para #4 and 6) which reads on the applicant's use of the term "multiple-use identification" ("Appliance ID 210 is a serial number, phone number, security code, or other

suitable unique identifier, of the cell phone 102 that uniquely identifies cell phone 102. Accordingly, the appliance ID 210 is referred to herein as a multiple-use unique identifier since the appliance ID 210 uniquely identifies the appliance and identifies the appliance as an authorized device to embodiments of the private database wireless access system”).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the appliance ID is multiple-use identification indicia that is included in all communications from the wireless communication device, to provide means for an ID to have multiple uses (ie. used as a phone number, security check, etc.)

As per **claims 3, 14 and 26**, Garrison teaches claim 2/13/25 **but is silent on** wherein the multiple-use identification indicia and the security indicia correspond to a telephone number of the wireless communication device.

Rezvani teaches authenticating a user via an ESN number of a cellular phone (Para #4 and 6) which reads on using the telephone number/MIN of the phone since both uniquely identify the user and can be used interchangeably.

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that wherein the multiple-use identification indicia and the security indicia correspond to a telephone number of the wireless communication device, to provide for associating a user to their phone for security purposes (eg. that one user will use that one phone).

As per **claim 4**, Garrison teaches claim 1 **but is silent on** wherein the appliance ID is a unique identifier included in a header information of the private database access request from the received wireless communication device.

Rezvani teaches transmitting data/header to a remote system that includes transmission of information including identification information (Para#66 and figure 4, #254/#258).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that the appliance ID is a unique identifier included in a header

information of the private database access request from the received wireless communication device, to provide means for transmitting the appliance ID in the overhead of a message header.

As per **claim 5**, Garrison teaches claim 1, wherein communicating further comprises transmitting the information radio frequency (RF) signal to the wireless communication device.

As per **claim 6**, Garrison teaches claim 1, wherein receiving the private database access request further comprises receiving information selecting one of a plurality of different private databases wherein the selected private database is communicated to the wireless communication device when the appliance ID corresponds to the security indicia (figures 4a-b teach the user being verified and then having access to databases, figure 1, 20a-d).

claims 7-11: recently objected to as containing novel material.

claim 18: recently objected to as containing novel material.

As per **claims 15-16**, Garrison teaches claim 13, further comprising;
receiving a second private database access request from a second wireless communication device (Para #3 teaches authorized access by users), the second private database access request including at least a password generated by a user (Para#42);

comparing the received password with a security code, the security code uniquely associated with the user (Para#42); and

but is silent on associating a second security indicia with a second unique appliance ID of the second wireless communication device when the received password corresponds to the security code, so that the private database is communicated to the second wireless communication device.

Garrison teaches authenticating a user via username and password, as pointed out by the primary examiner above. Garrison discloses use of many different communications networks (see Para#33) and one skilled understands that this would encompass use of the Internet. Hence the client's device/computer would use TCP/IP addressing which would inherently uniquely identify the appliance ID.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access a (remote) database via communication means (Para#'s 108-111, 113 teaches cellular phone access, 121, 122 and 134).

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that associating a second security indicia with a second unique appliance ID of the second wireless communication device when the received password corresponds to the security code, so that the private database is communicated to the second wireless communication device, to provide means for the system to support access by a plurality of users based on their device ID and/or login/password.

As per **claim 17 and 29**, Garrison teaches claim 12/27 **but is silent on** further comprising:

selecting a portion of the received private database using a browser, and
displaying the selected portion of the received private database on a display
residing on the wireless communication device using the browser.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access and view a (remote) database via communication means (Para#'s 108-111, 113 teaches cellular phone access, 121, 122 and 134). Note Para#108 specifically teaches "...client device 22 may include, for example, an Internet browser application that may be used to access web pages via communications network 16".

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that selecting a portion of the received private database using a

browser, AND displaying the selected portion of the received private database on a display residing on the wireless communication device using the browser, to provide support for Internet access.

As per **claim 20**, Garrison teaches claim 19, further comprising a memory configured to store the received private database (figure 2 is the client device which comprises a memory, #22).

As per **claim 21**, Garrison teaches claim 19, further comprising:
a display (figure 2, #29) **but is silent on** a browser configured to display the received private database on the display.

Rezvani teaches using a cellular phone's ESN to uniquely identify and register an user (Para#4). Rezvani teaches the user may access and view a (remote) database via communication means (Para#'s 108-111, 113 teaches cellular phone access, 121, 122 and 134). Note Para#108 specifically teaches "...client device 22 may include, for example, an Internet browser application that may be used to access web pages via communications network 16".

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that it uses a browser configured to display the received private database on the display, to provide means for access via the Internet.

As per **claim 23**, Garrison teaches claim 22 further comprising security code corresponding to a user associated with the private database, so that when the received ID is not initially associated with the security indicia, a password provided by the user of the remote wireless communication device causes the multiple-use unique ID to be associated with the security indicia when the password corresponds to the security code (Para#42 teaches use of login/password which is associated with the user's device).

As per **claim 28**, Garrison teaches claim 27 further comprising transmitting via both Internet and RF communications, the information from the remote database to the PWCD (figure 1 and Para #33 shows connections from the user to the remote database. Since Garrison teaches both wired/wireless technology, one skilled understands that the mobile user will send an RF message which will eventually be connected to a wired/Internet connection that connects to the database server).

Claim 32 rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison/Rezvani/(Shimada or Wilber or Khouri or Obouchi or Ronen or Yamazaki). and further in view of Schneider et al. US 6,178,505.

As per **claim 32**, Garrison teaches claim 27 comprising authenticating, without a user of the PWCD entering a password, whether the PWCD is authorized to access the information stored in a remote database.

Schneider teaches authentication, albeit poor, via just an IP Address:

As is clear from the above list of identification information, the degree to which a firewall can trust identification information to authenticate a user depends on the kind of identification information. For example, the IP address in a packet can be changed by anyone who can intercept the packet; consequently, the firewall can put little trust in it and authentication by means of the IP address is said to have a very low trust level. On the other hand, when the identification information comes from a token, the firewall can give the identification a much higher trust level, since the token would fail to identify the user only if it had come into someone else's possession. (C3, L16-27)

It would have been obvious to one skilled in the art at the time of the invention to modify Garrison, such that a password is not required, to provide means for different levels of security.

(10) Response to Argument

1. As stated previously, the USC 112 rejection has been overcome.
2. As stated previously, the examiner has determined that several claims now stand objected to as containing novel material. **These claims are 7-9, 10-11 and 18.**
3. The appellant's first argument focuses on the teachings of the prior art claiming they do not establish a prima facie case (eg. there is not motivation to combine) and hindsight is used.

Claim 1 is shown below:

1. (currently amended) A method for **communicating information from a private database to a wireless communication device**, the method comprising:
receiving a private database access request from the wireless communication device, the private database access request **including at least an appliance identification (ID) that uniquely identifies the wireless communication device;**
comparing the appliance ID with a security indicia, the security indicia associated with the wireless communication device; and
communicating the information from the private database to the wireless communication device when the appliance ID corresponds to the security indicia, **wherein verification of only the appliance application ID is sufficient to authorize access to the private database.**

The examiner must give each claim presented it's broadest reasonable interpretation. To summarize the claim (**see bold font above**), it merely states that a mobile user will access a remote server's database by using an "appliance ID" to identify the device whereby said ID is then compared to known values (eg. security indicia database) and access is either granted or denied.

a) Firstly, the examiner contends that an "appliance ID" is not a well known industry-standard term and is used by the applicant to broaden it's claims. Their Figures 1 and 2 show a web-enabled cell phone connecting thru the Internet to a database server. In doing this, the examiner notes that an Internet connection inherently requires an IP Address to be assigned (which reads on an "appliance ID").

Secondly, an IP Header inherently includes (in each and every packet sent) the Source and Destination Addresses (eg. the cell phone's address and the remote server's address).

Thirdly, the technology for allowing a remote user (eg. employee) to dial into a (company's) network, perhaps while on travel, has existed for considerable time. The examiner stated in his FINAL Office Action (dated 11-7-2005) that Remote Access is a well known technology and companies such as Shiva, Microsoft, Cisco, Nortel, etc. all sell Remote Access Server (RAS) systems that provide remote access. These

“server/routers” have Access Lists that can be programmed (by IT Department personnel) such that only a range (or ranges) of IP Addresses will be allowed to gain entry to the network/servers. Hence this is an IT Department’s first defense against hackers – other well known devices include Firewalls, Proxy servers, Screening Routers, etc.. Therefore, one skilled inherently expects at least one credential to be presented before access is granted. This “credential” can relate to hardware-specific information (eg. an IP Address, MAC Address, Phone Number/ESN, etc.) and/or to user-specific information such as a Username login, PIN, etc.. Therefore the examiner interprets that an IT Department will, when assigning IP Addresses to these wireless devices, either keep track of them and use them in a database as a “first-level” check when allowing a person attempting access to proceed with any additional checks (eg. log-in and password) and/or create access lists, which depends on how much security is warranted by the company.

➤ Based on this knowledge itself, it appears the appellant’s claims merely disclose an access method that only “screens/filters” at layer-3 of the OSI Model (eg. the network layer) which is where a router/RAS Server “operates/filters”. Hence a router with an access list set up to allow the company’s range of IP addresses access to the remote database clearly reads on the claims.

Fourthly, the examiner notes that servers can provide multiple functions, eg. can have several software packages loaded onto them, and therefore an IT Department might implement a multiple software packages onto one server, eg. a RAS Program and a database program to reduce costs, number of servers, etc.. Examples of this are the well known Microsoft Office which provides WORD, EXCEL, POWER POINT and EMAIL programs which can be loaded onto one server. Hence one skilled would take the above information and implement a combined RAS/Database server – note that the number of users using the RAS and Database servers will have a “loading effect” and could dictate that they be separated onto different physical servers.

b) The examiner also asks the question, “do systems today blindly allow any device to make contact with an internal system without requiring some type of credential?”. While one might say “YES”, eg. Internet web sites do allow unverified access to home pages at a superficial level, the predominant answer would be “NO”. Additional security “checks” are always required when gaining access to user-specific data such as names, addresses, account numbers, credit information, etc.. Since the applicant’s claims are broadly written, one skilled can assume that their “wireless device” can be used by an employee of a company, perhaps on travel, who wishes to gain access to home-office systems such as email, databases, files, etc..

As a further example, one skilled expects that a large commercial company will spend tens/hundreds of thousands of dollars for a system that requires several credentials (eg. hardware ID, log-in, password, etc.) while a small company will look for an inexpensive/free alternative so that their RAS Server (eg. router) only checks IP addresses. Further to this point, the examiner believes that one unskilled in Remote

Art Unit: 2617

Access and Security Systems may offer a “poor” security design that only checks the hardware/appliance ID, but this would be easily spoofed since the IP Address can be assigned by the actual device user. That’s why Garrison teaches a more elaborate design – eg. to make it difficult for hackers to gain access.

Lastly, just because the appellant characterizes Garrison’s design as being “more elaborate” (eg. keys are exchanged), the examiner notes that this “more elaborate system” fully reads on their less-enabled system. One skilled can inherently see that Garrison’s disclosure of using the Internet reads on filtering on device ID (eg. IP Addresses), but he then goes on to further secure his network by using additional filtering (eg. keys, logins, passwords, etc.). The examiner believes this is akin to a car that can achieve 50mph reading on a car that achieves only 10mph. The 50mph car reads on the 10mph car, not the other way around. Therefore Garrison provides considerably more protection and his use of the Internet brings into play the use of screening on IP Addresses (eg. appliance ID’s).

Now lets review the examiner’s prior art or record:

I) The first sentence of Garrison’s Abstract states “A secure client/server system allows remote access to a database without allowing unauthorized users to access data stored on the database system”. This broad statement clearly and fully teaches the applicant’s independent claims except that it doesn’t specify a “design” for how the security is implemented. One skilled, or even one not skilled, could rattle off many different concepts of basic security that have become commonplace in our everyday life, to include log-ins, passwords, PINs, personal ID numbers (eg. account number, credit card number, SS#, etc.). While these reflect data memorized by the user (eg. not hardware-specific), there are other well known security measures that request the identity of the device, such as phone number on cellular accounts, Caller ID, Magnetic Card Readers that read the card which is inserted to determine the identity of the card, IP and MAC addresses which are configured on devices, etc.. Hence, the examiner could have considered Garrison as a USC 102 piece of art since he clearly has contemplated the need to request identification data from the user.

Looking at the prior art, Garrison teaches a client user (figure 1, #14) who securely accesses a remote database (#19a or #19b) via a communications network (#18). Garrison clearly states that the “communications network” can be a wireless network since Para #33 states the “the communications network can comprise any conventional communications networks or combination of networks such as, but not limited to, the PSTN, cellular network, etc...”. Para #16 states that a mobile user/client transmits a password to the remote server to identify the user as an authorized user. Therefore, the examiner believes Garrison clearly teaches a wireless user who securely connects to a remote server using security means.

Next, and seemingly most importantly, appellant’s claim 16 explicitly states that a password is not required:

16. (previously presented) The method of claim 12, further comprising granting access to the private database without requiring a user of the wireless communication device to enter a password.

Hence one can assume that the appellant was cognizant of using a password but then considered removing this need (eg. weakened security for quick access). In doing this, the examiner interprets that Garrison relies (at minimum) on the IP Address of the mobile device as being recognized by the remote server (which again is inherent in IP Packet transfers) and that one can build upon this one piece of verification by adding more checks/balances (such as Garrison's key exchange, or PINs, passwords, log-ins, etc.). Furthermore, the examiner believes the applicant is cognizant of an "appliance ID" being supplied in an IP Packet because claim 4 explicitly states that the appliance ID will be contained in the header of the data transmitted/received:

4. (original) The method of claim 1, wherein the appliance ID is a unique identifier included in a header information of the private database access request from the received wireless communication device.

Hence, the examiner can interpret that the appellant simply read Garrison's design and removed certain "extra" security measures and then argues that Garrison teaches such an elaborate system that Garrison has not contemplated using just the appliance ID. The appellant's argument is akin to saying that a car which drives at 50mph does not read on a car that can drive at 10mph. Similarly, Garrison/Rezvani can simply use only the sender's appliance ID (eg. IP address, MAC Address, phone number, ESN, etc.) to gain access to a remote database since the security measures can be varied (eg. lowered/increased) as desired while staying within the bounds of Garrison/Rezvani's teachings without exceeding the technical aspects of those teachings.

II) The appellant's term "appliance ID" is open to interpretation since it is not a well known, "specific term" used in industry (eg. there is no such thing as an "appliance ID" which means one-and-only-one thing as compared to a router, mux or transceiver).

a) The examiner therefore puts forth at least one interpretation of the appliance ID as reading on a TCP/IP connection since each IP Packet inherently provides the sender's IP Address (which reads on the "appliance ID" since a computer/appliance must be assigned an IP address in order for it to connect to a TCP/IP network).

b) Should the mobile-to-server link be a wired/wireless "LAN connection" in that it does not need to cross multiple routers (eg. a WAN connection), the MAC address of the mobile device would remain unchanged and also read on the appliance ID (the examiner notes that a packet that needs to cross multiple routers will have the original sender's MAC Address changed, but as stated in B1 above, the IP Address will always remain as the sender's IP Address).

Art Unit: 2617

c) The examiner can also interpret that the use of only one piece of data to allow access reads on a single sign-on concept (eg. one secure piece of information gets you access to all systems instead of having to remember multiple passwords). Hence, the appliance ID would allow network access to all systems. While this is convenient, it is also “dangerous” since a hacker will have total access should they steal the device and/or password.

d) The examiner’s rejection did not rely on examples B1, B2 or B3 above, but provided multiple references to show that the use of a device’s hardware address (eg. interpreted as a phone number or ESN number) was well known in the art as well.

The examiner therefore disagrees with the appellant’s characterization of Garrison’s teachings since they disparage Garrison by delving down into his specific teachings. The examiner is not concerned that Garrison teaches a more elaborate key-transfer for connections, he is using Garrison as a primary piece of prior art to show that providing a secure connection between a wireless user to a remote database server has been previously contemplated and that “security information” is sent and compared for access. All that is “lacking” is an explicit teaching of determining the user/appliance ID and if one skilled would require this piece of information during authentication. Since **a)** the examiner is well aware of many prior art systems that authenticate a user based on the device they are using in conjunction with user credentials (eg. A computer’s TCP/IP Address along with a User’s Log-in and Password respectively) and **b)** Garrison teaches a secure remote wireless connection, the examiner merely needs to show other prior art references that explicitly teach using an appliance ID.

- Note: Since Garrison discloses a connection using the Internet (Para. 33) the appellant would not be afforded an interpretation whereby they securely connect a user to a database whereby the appliance ID is a TCP/IP Address, since this would read on Garrison.

Renzavi was added since he discloses a cellular device uses its ESN (eg. appliance ID) when authenticating/registering. Renzavi further discloses (see figure 9) that “a client device....connects to the Internet.....may be any device suitable for communicating with the remote site via communications network.....the link may include dial-up, satellite link, or any other suitable communications link or combination of communication links.....remote site may include one or more servers, for example web server, database server....dynamic web pages supplied by database server may be viewed by a user...” (See paragraphs 108-111). Furthermore paragraph 113 teaches remote user access devices may include PDA’s, cellular phones, computers or any other suitable device. Hence, taken at a high-level, Renzavi clearly teaches remote access for cellular devices whereby an ESN would be transmitted for authentication.

The examiner then provided six more differing pieces of art (in the alternative) which put forth specific teachings of an access system that uses (at least) a phone number during authentication (most/all are not specifically addressed in-depth by the

appellant). The examiner believes that, while this number of references is excessive, it was used to clearly show and reinforce that this idea is well known and popular. One can envision many of these designs being used in the early days of dial-up Internet service whereby the user simply dialed their ISP's phone number (eg. a modem bank) and the caller's phone number was verified as being an ISP customer, hence said user was assigned a modem thereby granting a data connection to the Internet. This "design" has disappeared for countless/millions of Internet users since the inception of cable modems whereby the Internet connection is virtually "always on" (eg. the link is extended from the cable provider to the user's house so there is "conceptually" no need to verify the user since there is no middle-man). The old design, previously described, had the user connecting to the ISP through the PSTN (who was not verifying the person), hence the ISP would desire a quick authentication process (eg. verify the caller's ID/Phone number).

This same idea can be applied to remote wireless access since the cellular network is akin to the PSTN just described, eg. they are not verifying that the person dialing into the database server. Hence a company's IT Department sets up a remote access server (RAS) with a database of the phone numbers (eg. appliance ID's) of trusted devices (eg. company employees).

As another point of disagreement, the combination of Garrison and Rezvani provide a more robust security design since Garrison does in fact disclose using more than one piece of information to authenticate a user. But one skilled, who considers the evolution of technical systems, would be apt to conclude that initial security systems used only one piece of data to verify a user – as systems were compromised/hacked, IT departments required more secure systems (eg. key exchanges, log-ins, passwords, randomly generated ID's such as RSA's SecurID, etc.). Therefore the Garrison/Rezvani system can be viewed as providing any/all levels of security that are disclosed, eg. low-security using only one piece of data (eg. appliance ID) and high(er) security using passwords, log-ins, key exchanges for those who access highly important data.

The applicant states (pages 11-12):

"..For at least the following reasons, no suggestion or motivation exists to modify or combine Garrison in view of Rezvani. First, Applicant argues that no teaching or suggestion exists to make the combination because the references are directed to completely different art and completely unrelated inventions. Garrison is directed to establishing a secure connection between a client computer and a server computer so the client can safely and securely access a database (see [0014]). In Garrison, a new encryption key is used for each new data session to inhibit unauthorized users (i.e., hackers) from accessing the database (see [0042]). By contrast, Rezvani is directed to automatically detecting a wireless device and registering the wireless device with a controller (see [0055], Abstract, and Summary)..."

Art Unit: 2617

How can the appellant say the prior art does not teach the claim when Garrison fully discloses virtually 99% of what they are claiming, eg. secure wireless remote access to a database? Also, the examiner fully disagrees with the appellant's characterization that the two pieces of art "solve completely different problems". The motivation to use an ESN number has been known and used for considerable time and one skilled can/would use it to uniquely identify the device (similar to using an IP Address, as taught by Garrison).

It is the examiner's opinion that the appellant is attempting to convolute the rejection by using extreme details of Rezvavi's design to overcome the prior art. While Rezvavi may consider "...tracking wireless devices and the problems of clock drift between controllers and transmitters", the examiner cited specific paragraphs (previously listed) to show that Rezvani fully contemplates a remote user connecting to a database using a cellular device (whereby authentication would use the ESN number of the phone). Hence the examiner is not using Rezvani for "just any reason", but rather to specifically show that prior art has contemplated that a appliance ID, eg. phone number in this case, would be verified before a connection is allowed to a remote server.

Furthermore, the appellant is attacking the references singularly when a USC 103 combination has been put forth. Garrison teaches everything that is needed except for an "explicit" use of an appliance ID (although it could be interpreted as an IP Address). Hence, there is no need for Rezvani to support those claim limitations, only that he discloses secure access means using an appliance ID (eg. ESN), which he does.

As a last point, the examiner notes that the appellant has not fully considered that if the prior art uses a TCP/IP-enabled device and connection (as disclosed in Garrison), it will fully read on their claims since the device's IP Address (eg. appliance ID) is transmitted in each packet. The appeal brief is remiss by not addressing this point. It is the examiner's position that this would have been a more persuasive strategy/argument since it would stand to rebut the technical merits of prior art.

III. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

This is clearly not the case since the prior art (Garrison) teaches virtually each independent claim singularly (eg. securely connecting to a remote database) while Rezvani (and the many others) are used to explicitly teach using an address ID/phone number as "a credential" that is verified.

Art Unit: 2617

IV. The appellant then argues that Rezvani's "automatic sensing/registration" negates the combination and therefore no reasonable expectation of success will occur. The examiner respectfully disagrees for several reasons; a) making a manual process "automatic" is not novel unto itself, b) Garrison teaches everything in the claims except for using the appliance ID, so the "concept" of using an ESN to authenticate a user can be gleaned from Rezvani's teachings and applied to other, more different processes. The applicant attempts to require that "everything" taught by Rezvani must be combined with Garrison when this is not true – eg. Garrison's deficiency is cured by Rezvani by taking his concept of using an ESN number as a "credential" that would be transmitted to the remote site during authentication.

More specifically, the arguments boil down to "a security and authentication process".

A basic process would be:

- a. User contacts remote site
- b. Remote site asks for credentials
- c. User sends credentials
- d. Remote site validates credentials
- e. User is either granted or denied access.

Garrison's design (or inventive concept) teaches this very process. Where there is "deviation" from the appellant's design is in the details of "step c", eg. sending the credentials. An authentication process can verify many different facts about the user in order to grant/deny access. One skilled understands that the credentials can be log-in, password, the location of the user, the time access is attempted, biological factors, and even hardware related credentials such as IP Address, MAC Address, appliance ID, etc.. Therefore, at the very least, one can require a "physical" credential to verify the device which is seeking access – in fact, it would be virtually impossible for two computer devices to "talk to each other" blindly without understanding at the hardware level who each device is (eg. based on IP Addresses). Rezvani (and the many other patents listed) provide this teaching and one skilled understands that, at a high level, many different credentials can/may be used when setting up the process for tight, foolproof security.

V. Regarding "All elements not being taught" (page 14), the appellant argues that using only the appliance ID is not taught. Firstly, the examiner notes that the "level of security" can be varied based on the importance of the data being safeguarded. Secondly, even before a user attempting to gain access to the remote sight can type a character, the two devices have exchanged "hardware/appliance IDs" via the communications link such that they know who and where to send the request data. It would be remiss of the appellant to think that Garrison allows the mobile and server devices to "blindly" connect when the IT department has assigned the IP Address of the mobile device and it would be known (eg. well known devices such as RAS Servers, Screening Routers, Firewalls and Proxy Servers inherently check the IP Address of any device attempting to gain access).

The prior art cited provides considerably more security than the appellant and thus would have used only an appliance ID many “generations” ago, meaning authentication processes have evolved from “verifying through an in-person visit” (eg. when using a notary) to remotely authenticating a user (eg. such as taught by Garrison). Hence the Garrison/Rezvani combination can provide the security process disclosed and any subset requiring “less” than that disclosed (eg. user provides less credentials) but the examiner cannot assume that Garrison/Rezvani would provided “more” security.

It is therefore the examiner’s position that Garrison/Rezvani can provide using only the appliance ID whereby any more required security checking is at the user’s discretion.

VI. Independent claims 1, 12, 19, 22, 24, 25 and 27 (Page 14): The applicant argues that only the appliance ID is sufficient. Garrison teaches using the Internet which would require IP Packets that inherently show the sender’s address/ID. Devices such as Firewalls, Proxys, Screening routers contain IP Database’s to identify authorized personnel. Garrison/Rezvani teach a more robust system, but at a minimum, some piece(s) of data must be exchanged before a user will be granted access. Also, the appellant is attacking the references individually. In response to applicant’s arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). They ask that Rezvani teach using an ESN to access a database, but that would essentially require the examiner to find a USC 102 rejection (eg. Garrison teaches securely accessing a database whereas Rezvani teaches an ESN is used for authentication). The USC 103 combination clearly reads on the claims.

VII. Response to Office Action (page 15-26): The appellant provides many pages which re-argue the arguments made above. Therefore the examiner believes these to have been answered – eg. the prior art does not teach away, since the combination fully reads on the claims, hindsight is not used, a prima facie case has been established and motivation exists to explicitly teach using an appliance ID such as an IP Address, Phone number/ESN, etc..

Summarizing, the prior art teaches a process by which a user can securely access a remote database via a wireless link. Security “processes” are well known in the art and range from requiring at least one basic credential to requiring many different credentials, so the examiner must determine if the claimed process itself is novel.

It is his belief that the prior art provides a more robust, more secure access design which is an “evolution” from the more limited, more basic design claimed by the appellant. Hence, “early” access systems provided a design whereby only one piece of information was required (eg. either device-related or user-related) and these basic systems are well known in the art.

The appellant has continually and conveniently disregarded the fact that Garrison’s teachings support TCP/IP connectivity (eg. the Internet can be used), hence

Art Unit: 2617

IP Packets inherently disclose the sender's hardware device address (eg. appliance address) – not to mention login, password, keys, etc.. Therefore the examiner believes the prior art to anticipate each and every limitation as written in the claims (except for those shown as novel). Garrison teaches a secure connection from a wireless user to a remote server but is missing an explicit "security verification" that uses a device ID. Rezvani explicitly teaches using a phone number/ESN for gaining entry to a system. Therefore Garrison's teachings can be modified such that his security verification process uses an ESN.


For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Stephen D'Agosta

Primary Examiner

STEVE M. D'AGOSTA
PRIMARY EXAMINER


11-2-06

Conferees:

William Trost

SPE



WILLIAM TROST
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600

Joseph Field

SPE



JOSEPH FEILD
SUPERVISORY PATENT EXAMINER